Search Results

Search Results for: **[protocol analyzer]**
Found **40** of **114,152 searched.**

Search within Results

1 A study of protocol analysis for packet switched network 100

K. Tsukamoto , T. Itoh , M. Nomura , Y. Tanaka

Proceedings of the seventh data communications symposium October 1981

Communication failures may occur because of residual hardware or software implementation flaws, operator errors, transmission noises and transient or permanent machine failures. For packet switched network operation, some means are necessary to detect the errors and to analyze the phenomena to identify the causes of the errors, since, generally, it is almost impossible to predict errors or to implement systems without errors or failures. This paper describes general aspects of co ...

2 A network protocol analyzer with tutorial 100

Susan Mengel , Salman Ali

Proceedings of the 1996 ACM symposium on Applied Computing February 1996

3 Visualizing packet traces 96%

John A. Zinky , Fredric M. White

ACM SIGCOMM Computer Communication Review , Conference proceedings on Communications architectures & protocols October 1992

Volume 22 Issue 4

This paper describes an environment for visualizing packet traces that greatly simplifies troubleshooting protocol implementations. Network management centers routinely collect packet traces to tally traffic statistics and to troubleshoot protocol configuration and implementation problems. Previous efforts have focused on the reliable collection of traces and their statistical interpretation. Display of packet traces was restricted to a textual representation of the raw headers. Our prototy ...

4 Group Key Management and Signatures: Formalizing GDOI group key management requirements in NPATRL 96%

Catherine Meadows , Paul Syverson

Proceedings of the 8th ACM conference on Computer and Communications Security November 2001

Although there is a substantial amount of work on formal requirements for two and three-party key distribution protocols, very little has been done on requirements for group protocols. However, since the latter have security requirements that can differ in important but subtle ways, we believe that a rigorous expression of these requirements can be useful in determining whether a given

protocol can satisfy an application's needs. In this paper we make a first step in providing a formal understan ...

5 ATM test-bed architecture for training purposes 91%

Rana Ejaz Ahmed

International Journal of Network Management January 2001

Volume 11 Issue 1

Due to the recent tremendous growth in ATM products, there is a strong need for training and education for engineers working in the field of ATM networks. This paper describes the architecture of an ATM test-bed that can be used to provide such traiing. Copyright © 2001 John Wiley & Sons, Ltd.

6 ASN.1 protocol specification for use with arbitrary encoding schemes 87%

Duke Tantiprasut , John Neil , Craig Farrell

IEEE/ACM Transactions on Networking (TON) August 1997

Volume 5 Issue 4

7 Focus on AiroPeek 85%

Gilbert Held

International Journal of Network Management August 2002

Volume 12 Issue 5

8 Verifying security protocols as planning in logic programming 84%

Luigia Carlucci Aiello , Fabio Massacci

ACM Transactions on Computational Logic (TOCL) October 2001

Volume 2 Issue 4

We illustrate *ALSP* (Action Language for Security Protocol), a declarative executable specification language for planning attacks to security protocols. *ALSP* is based on logic programming with negation as failure, and with stable model semantics. In *ALSP* we can give a declarative specification of a protocol with the natural semantics of send and receive actions which can be performed in parallel. By viewing a protocol trace as a plan to a ...

9 A compiler for analyzing cryptographic protocols using noninterference 84%

Antonio Durante , Riccardo Focardi , Roberto Gorrieri

ACM Transactions on Software Engineering and Methodology (TOSEM) October 2000

Volume 9 Issue 4

The Security Process Algebra (SPA) is a CCS-like specification languag e where actions belong to two different levels of confidentiality. It has been used to define several noninterference-like security properties whose verification has been automated by the tool CoSeC. In recent years, a method for analyzing security protocols using SPA and CoSeC has been developed. Even if it has been useful in analyzing small security protocols, this method has shown to be error-prone, as it requires the ...

10 Session 2A: embedded tutorial: Challenges and opportunities in broadband and wireless communication designs 82%

Jan M. Rabaey , Miodrag Potkonjak , Farinaz Koushanfar , Suet Fei Li , Tim Tuan

Proceedings of the 2000 IEEE/ACM international conference on Computer-aided design November 2000

Communication designs form the fastest growing segment of the semiconductor market. Both network processors and wireless chipsets have been attracting a great deal of research attention, financial resources and design efforts. However, further progress is limited by lack of adequate system methodologies and tools. Our goal in this tutorial is to provide impetus for development of communication design techniques and tools.The first part addresses network processors (NP) that we study from three v ...

11 Verifying security protocols with Brutus 82%

E. M. Clarke , S. Jha , W. Marrero

ACM r ns cti ns n ftw re Engineering nd Meth d l gy (O EM) Oct ber 2000

Volume 9 Issue 4

Due to the rapid growth of the "Internet" and the "World Wide Web", security has become a very important concern in the design and implementation of software systems. Since security has become an important issue, the number of protocols in this domain has become very large. These protocols are very diverse in nature. If a software architect wants to deploy some of these protocols in a system, they have to be sure that the protocol has the right properties as dictated ...

12 Formal verification of standards for distance vector routing protocols 80%

Karthikeyan Bhargavan , Davor Obradovic , Carl A. Gunter

Journal of the ACM (JACM) July 2002

Volume 49 Issue 4

We show how to use an interactive theorem prover, HOL, together with a model checker, SPIN, to prove key properties of distance vector routing protocols. We do three case studies: correctness of the RIP standard, a sharp real-time bound on RIP stability, and preservation of loop-freedom in AODV, a distance vector protocol for wireless networks. We develop verification techniques suited to routing protocols generally. These case studies show significant benefits from automated support in reduced ...

13 Automated protocol verification in linear logic 80%

Marco Bozzano , Giorgio Delzanno

Proceedings of the Fourth ACM SIGPLAN Conference on Principles and Practice of Declarative Programming October 2002

In this paper we investigate the applicability of a bottom-up evaluation strategy for a first order fragment of linear logic [7] for the purposes of automated validation of authentication protocols. Following [11], we use multi-conclusion clauses to represent the behaviour of agents in a protocol session, and we adopt the Dolev-Yao intruder model and related message and cryptographic assumptions. Also, we ...

14 Increasing the observability of Internet behavior 80%

Thomas M. Chen

Communications of the ACM January 2001

Volume 44 Issue 1

15 Securing a global village and its resources: baseline security for interconnected signaling system #7 telecommunications networks 80%

Hank M. Kluepfel

Proceedings of the 1st ACM conference on Computer and communications security December 1993

The resulting national focus on Network Integrity issues, spawned the development of an industry commitment to affect and realize a minimum security baseline for interconnected SS7 networks. In addition the affected carriers in those outage have accelerated their pursuit of secure solutions to today's intelligent networking.[2]This paper will focus on the development of the baseline and the current effort to take the baseline into national, e.g., National Ins ...

16 Paradigm shifts in protocol analysis 77%

Susan Pancho

Proceedings of the 1999 workshop on New security paradigms September 1999

17 Measurements of DCE RPC performance in an OS/2 environment 77%

Ying Sun , Rick Bunt , Greg Oster

Proceedings of the 1996 conference of the Centre for Advanced Studies on Collaborative research November 1996

Developing and managing applications for environments consisting of independently configured computing systems interoperating across network connections is of considerable interest in the commercial sector and presents many research challenges. The Open Software Foundation's Distributed Computing Environment (DCE) has evolved to address the need for a vendor-neutral platform to which distributed applications can be developed. Central to the design philosophy of DCE is its reliance on the Remote ...

18 Session 5: P2P and streaming: MediaPlayer™ versus RealPlayer™: a comparison of network turbulence 77%

Mingzhe Li , Mark Claypool , Robert Kinicki

Proceedings of the second ACM SIGCOMM Workshop on Internet measurment workshop November 2002

The performance of currently available streaming media products will play an important role in the network impact of streaming media. However, there are few empirical studies that analyze the network traffic characteristics and Internet impact of current streaming media products. This paper presents analysis from an empirical study of the two dominant streaming multimedia products, RealNetworks RealPlayer™ and Microsoft MediaPlayer™. Utilizing two custom media player measurement tool ...

19 Key management and key exchange: Efficient, DoS-resistant, secure key exchange for internet protocols 77%

William Aiello , Steven M. Bellovin , Matt Blaze , John Ioannidis , Omer Reingold , Ran Canetti , Angelos D. Keromytis

Proceedings of the 9th ACM conference on Computer and communications security November 2002

We describe JFK, a new key exchange protocol, primarily designed for use in the IP Security Architecture. It is simple, efficient, and secure; we sketch a proof of the latter property. JFK also has a number of novel engineering parameters that permit a variety of trade-offs, most notably the ability to balance the need for perfect forward secrecy against susceptibility to denial-of-service attacks.

20 Cryptographic protocols: The verification of an industrial payment protocol: the SET purchase phase 77%

Giampaolo Bella , Lawrence C. Paulson , Fabio Massacci

Proceedings of the 9th ACM conference on Computer and communications security November 2002

The Secure Electronic Transaction (SET) protocol has been proposed by a consortium of credit card companies and software corporations to secure e-commerce transactions. When the customer makes a purchase, the SET dual signature guarantees authenticity while keeping the customer's account details secret from the merchant and his choice of goods secret from the bank.This paper reports the first verification results for the complete purchase phase of SET. Using Isabelle and the inductive method, we ...

Search Results

Search Results for: **[protocol analyzer]**
Found **40** of **114,152 searched.**

Search within Results

21 ITiCSE 2000 working group reports: Support for teaching formal methods 77

Vicki L. Almstrum , C. Neville Dean , Don Goelman , Thomas B. Hilburn , Jan Smith

Working group reports from ITiCSE on Innovation and technology in computer science education June 2001

This report describes a growth path for the area referred to as *formal methods* within the computing education community. We define the term formal methods and situate it within our field by highlighting its role in Computing Curricula 1991, Computing Curricula 2001, and the SoftWare Engineering Body Of Knowledge (SWEBOK). The working group proposes an enhancement to an existing web resource, which is a rich collection of materials and links related to formal methods. The new resource is d ...

22 ITiCSE 2000 working group reports: Support for teaching formal methods 77

Vicki L. Almstrum , C. Neville Dean , Don Goelman , Thomas B. Hilburn , Jan Smith

ACM SIGCSE Bulletin June 2001

Volume 33 Issue 2

This report describes a growth path for the area referred to as *formal methods* within the computing education community. We define the term formal methods and situate it within our field by highlighting its role in Computing Curricula 1991, Computing Curricula 2001, and the SoftWare Engineering Body Of Knowledge (SWEBOK). The working group proposes an enhancement to an existing web resource, which is a rich collection of materials and links related to formal methods. The new resource is d ...

23 Supercomputer network selection: a case study 77

William L. French

Proceedings of the 1990 ACM/IEEE conference on Supercomputing November 1990

With the purchase of a Cray-2 supercomputer, Eli Lilly and Company (Lilly) needed a high performance network to provide communications with this computer. At the time of installation of the Cray, this network had to provide access from VAX/VMS computers using Cray Station software while also supporting communications from UNIX and other machines utilizing TCP/IP. The capability of access from other computers, especially IBM mainframes, was also desirable in the longer term. Finally, this network ...

24 An approach to finding the attacks on the cryptographic protocols 77

Yongxing Sun , Xinmei Wang

ACM SIGOPS Operating Systems Review July 2000

Volume 34 Issue 3

It is necessary to development the formal tools for verifying cryptographic protocols because of the subtlety of cryptographic protocols flaws; In terms of the notions of the restrictive channel and the equivalent message, this paper presents an approach that utilizes the substitution rules of messages and the deduction rules to prove whether the insecure states of the cryptographic protocols are reachable or not, and the analysis of several famous protocols shows the validity of the method.

25 Protocol Analysis: The faithfulness of abstract protocol analysis: message authentication 77

Joshua D. Guttman , F. Javier Thayer , Lenore D. Zuck

Proceedings of the 8th ACM conference on Computer and Communications Security November 2001

Dolev and Yao initiated an approach to studying cryptographic protocols which abstracts from possible problems with the cryptography so as to focus on the structural aspects of the protocol. Recent work in this framework has developed easily applicable methods to determine many security properties of protocols. A separate line of work, initiated by Bellare and Rogaway, analyzes the way specific cryptographic primitives are used in protocols. It gives asymptotic bounds on the risk of failures of ...

26 Behavioural analysis of the enterprise JavaBeans component architecture 77

Shin Nakajima , Tetsuo Tamai

Proceedings of the 8th international SPIN workshop on Model checking of software May 2001

Rigorous description of protocols (a sequence of events) between components is mandatory for specifications of distributed component frameworks. This paper reports an experience in formalizing and verifying behavioural aspects of the Enterprise Java Beans™ specification with the SPIN model checker. As a result, some potential flaws are identified in the EJB 1.1 specification document. The case study also demonstrates that the SPIN model checker is an effective tool for behavioura ...

27 Directed explicit model checking with HSF-SPIN 77

Stefan Edelkamp , Alberto Lluch Lafuente , Stefan Leue

Proceedings of the 8th international SPIN workshop on Model checking of software May 2001

We present the explicit state model checker HSF-SPIN which is based on the model checker SPIN and its Promela modeling language. HSF-SPIN incorporates directed search algorithms for checking safety and a large class of LTL-specified liveness properties. We start off from the A* algorithm and define heuristics to accelerate the search into the direction of a specified failure situation. Next we propose an improved nested depth-first search algorithm that exploits the structure of Promela Never ...

28 Dynamic analysis of security protocols 77

Alec Yasinsac

Proceedings of the 2000 workshop on New security paradigms February 2001

29 A quick check of network performance 77

Jeffrey T. Hicks , John Q. Walker

International Journal of Network Management January 2001

Volume 11 Issue 1

Have you ever tried to measure the response time across a network? Do you sometimes wonder what throughput rate you're getting over a particular link? Are you concerned about the impact of adding streaming multimedia traffic to a network? Would you like to know the exact route your data is taking? Individual tools are available to measure the throughput and response time of your applications, trace a network route, or test a network's capacity for handling ...

30 An overview of the center for wireless information network studies at Worcester Polytechnic Institute, MA, USA 77

Kaveh Pahlavan

ACM SIGMO ILE Mobile Computing and Communications Review April 2000

Volume 4 Issue 2

The Center for Wireless Information Network Studies (CWINS) is a well renowned compact wireless research laboratory with successful history of research alliances with other industrial and academic groups. The center has performed research for government agencies and has close ties with the world-leading organizations in the wireless industry. The core competence of the center is in indoor radio channel propagation measurement modeling and in the development of testbeds and tools for design and ...

31 Ignoring perfect knowledge in-the-world for imperfect knowledge in-the-head 77

Wayne D. Gray , Wai-Tat Fu

Proceedings of the SIGCHI conference on Human factors in computing systems March 2001

Memory can be internal or external - knowledge in-the-world or knowledge in-the-head. Making needed information available in an interface may seem the perfect alternative to relying on imperfect memory. However, the rational analysis framework (Anderson, 1990) suggests that least-effort tradeoffs may lead to imperfect performance even when perfect knowledge in-the-world is readily available. The implications of rational analysis for interactive behavior are investigated in two experiments. ...

32 The OpenView Enterprise Management Framework 77

Nathan J. Muller

International Journal of Network Management September 1996

Volume 6 Issue 5

In OpenView, Hewlett-Packard has concentrated on creating a multivendor management platform for TCP-IP-based internets. This plays to the company's strengths in LAN management, where it has been a major player in the LAN protocol analyzer market since the early 1980s, and its expertise in TCP/IP, which the company had been using internally since the early 1980s.

33 EtherPeek - Ethernet network analysis software 77

Gilbert Prem Held

International Journal of Network Management October 1998

Volume 8 Issue 5

34 A simple packet aggregation technique for fault detection 77

Akira Kanamaru , Kohei Ohta , Nei Kato , Glenn Mansfield

International Journal of Network Management July 2000

Volume 10 Issue 4

Packet monitoring has become a standard technique in network management and when applied to a large-scale transit network yields a high volume of packets. To overcome this problem, we discuss the behavior of packets and present a symptom-based packet aggregation technique which is useful for fault detection. Copyright © 2000 John Wiley & Sons, Ltd.

35 Clarifying straight replays and forced delays 77

Taekyoung Kwon , Jooseok Song

ACM SIGOPS Operating Systems Review January 1999

Volume 33 Issue 1

This paper clarifies straight replays which are one of replay attacks but have been somewhat misunderstood. There are various kinds of replay attacks on authentication protocols but most of the formal methods are not capable of detecting them because a replayed message may have appropriate data and structure for the protocols. [1] classified them and proposed their taxonomy that is useful for readily determining the effectiveness of some replay countermeasures and the appropriateness of analysis ...

36 Extending NCP for protocols using public keys 77

Aviel D. Rubin

Mobile Networks and Applications December 1997

Volume 2 Issue 3

One of the greatest obstacles to wide-spread deployment of wireless mobile systems is security. Cryptographically strong protocols and algorithms are required to enable secure communication over links that are easy to monitor and control by an attacker. While good cryptographic algorithms exist,

it is difficult to design protocols that are immune to malicious attack. Good analysis techniques are lacking. This paper presents extensions to a technique for specifying and analyzing nonmonotonic ...

37 Authentication services for computer networks and electronic messaging systems 77

Keok Auyong , Chye-Lin Chee

ACM SIGOPS Operating Systems Review July 1997

Volume 31 Issue 3

The paper surveys the authentication services used by modern computer systems and presents the major operational authentication services employed by commercial companies, banking as well as government departments. As distributed system services are susceptible to a variety of threats mounted by intruders as well as legitimate users of the system, password-based authentication is not suitable for use on computer networks.

38 An empirical evaluation of three methods for deadlock analysis of Ada tasking programs 77

James C. Corbett

Proceedings of the 1994 international symposium on Software testing and analysis August 1994

Static analysis of Ada tasking programs has been hindered by the well known state explosion problem that arises in the verification of concurrent systems. Many different techniques have been proposed to combat this state explosion. All proposed methods excel on certain kinds of systems, but there is little empirical data comparing the performance of the methods. In this paper, we select one representative from each of three very different approaches to the state explosion problem: partial-o ...

39 Data flow analysis of communicating finite state machines 77

Wuxu Peng , S. Puroshothaman

ACM Transactions on Programming Languages and Systems (TOPLAS) July 1991

Volume 13 Issue 3

40 Developing HP's Network Advisor using Smalltalk in a large project team 77

Tom Wisdom

ACM SIGPLAN OOPS Messenger , Addendum to the proceedings on Object-oriented programming systems, languages, and applications (Addendum) September 1991

Volume 3 Issue 4